Welcome to the PIA for FY 2011!

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

Directions:

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: http://vaww.privacy.va.gov/Privacy_Impact_Assessments.asp

Roles and Responsibilities:

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the VA Directive 6508 referenced in the procedure section of this document.

a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Directive 6508.

b. Records Officer is responsible for supplying records retention and deletion schedules.

c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Directive 6508 and to immediately report all anomalies to the Privacy Service and appropriate management chain.

d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.

e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and reviewing and approving the PIA before submission to the Privacy Service.

Definition of PII (Personally Identifiable Information)

Information in identifiable form that is collected and stored in the system that either directly identifies and individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirect indentify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

Macros Must Be Enabled on This Form

Microsoft Office 2003: To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

Microsoft Office 2007: To enable macros, go to: 1) Office Button > Prepare > Excel Options > Trust Center > Trust Center Settings > Macro Settings > Enable

All Macros; 2) Click OK

Final Signatures

Final Signatures are digitally signed or wet signatures on a case by case basis. All signatures should be done when all modifications have been approved by the VA Privacy Service and the reviewer has indicated that the signature is all that is necessary to obtain approval.

Privacy Impact Assessment Uploaded into SMART

Privacy Impact Assessments should be uploaded into C&A section of SMART.
All PIA Validation Letters should be emailed to christina.pettit@va.gov to received full credit for submission.

(FY 2011) PIA: System Identification

Program or System Name:	Region 1>VHA>VISN 19>Sheridan VAMC>VistA		
OMB Unique System / Application / Program Identifier		(AKA: UPID #):	029-00-01-11-01-1180-00
Description of System/ Application/ Program:	The VistA Legacy system runs on InterSystems Cache on VMS [VMS/Cache] platform and is located at		
Facility Name:	Sheridan Veterans Affairs Medical Center		

Title:	Name:	Phone:	Email:
Privacy Officer:	Jamie Banks	307.675.3611	jamie.banks@va.gov
Information Security Officer:	Doug Bohnenblust	307.675.3880	douglas.bohnenblust@va.gov
System Owner/ Chief Information Officer:	Cynthia Sostrom	307.675.3143	cynthia.sostrom@va.gov
Information Owner:			
Other Titles:			
Person Completing Document:	Nancy Snively	307.675.3798	nancy.snively@va.gov
Other Titles:			

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	05/2009
Date Approval To Operate Expires:	08/2011
What specific legal authorities authorize this program or system:	Title 38, USC, Section 7301
What is the expected number of individuals that will have their PII stored in this system:	60723 VA Personnel and 53502 patients
Identify what stage the System / Application / Program is at:	Operations/Maintenance
The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.	Operational 10 plus years
Is there an authorized change control process which documents any changes to existing applications or systems?	Yes
If No, please explain:	
Has a PIA been completed within the last three years?	Yes
Date of Report (MM/YYYY):	01/2011

Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form.

□ Have any changes been made to the system since the last PIA?

☑ Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?

☑ Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?

☑ Does this system/application/program collect, store or disseminate PII/PHI data?

☑ Does this system/application/program collect, store or disseminate the SSN?

If there is no Personally Identifiable Information on your system , please complete TAB 7 & TAB 12. (See Comment for Definition of PII)

(FY 2011) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records? If the answer above no, please skip to row 15.	Yes
For each applicable System(s) of Records, list:	
1. All System of Record Identifier(s) (number):	23VA16, 24VA19, 79VA19, 97VA105, 99VA13,121VA19
2. Name of the System of Records:	Information System and Technology Architecture (VistA-VA), Patient Medical Records, Non-VA Fee Basis Records, Consolidated Data Information System, Automated Safety Incident Surveillance and Tracking System, National Patient Databases
3. Location where the specific applicable System of Records Notice may be accessed (include the URL):	http://www.rms.oit.va.gov/SOR_Records.asp
Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?	Yes
Does the System of Records Notice require modification or updating?	No
	(Please Select Yes/No)
Is PII collected by paper methods?	Yes
Is PII collected by verbal methods?	Yes
Is PII collected by automated methods?	Yes
Is a Privacy notice provided?	Yes
Proximity and Timing: Is the privacy notice provided at the time of data collection?	No
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?	Yes
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?	No
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?	Yes

(FY 2011) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Paper	The most common data types that are captured and accessed on a regular basis by authroized individuals are first and last name, middle initial, DOB, SSN, and address. This patient informationfalls into two classes: administrative and clinical. Clinical Information is used to diagnose, prescribe treatment and follow clinically the patient through his/her health care encounters. Administrative data is used to identify the veteran (SSN), correspond to/from (name and address), and determine eligibility (patient administrative info + SSA and IRS data) and for payment of healthcare.	Verbally	Written
Family Relation (spouse, children, parents, grandparents, etc)	Paper	The information gathered will be used to determine eligiblity and will not be	Verbally	Written
Service Information	Paper	Military Service Information (Branch of service, discharge date, discharge type, service connection, medical conditions related to military service) This information is colleced to assess eligibility for VA healthcare benefits, type of healthcare needed.	Verbally	Written

Medical Information	Electronic/File Transfer	VistA-Legacy applications are used to meet a wide range of health care data needs. The system collects a wide range of personal medical information for clinical diagnosis, treatment, patient evaluation, and patient care. Common types of personal medical information would include lab test results, prescriptions, allergies, medical diagnosis, vital signs, etc. The information is used to treat and care for the veteran patient. Clinical information form VA and DoD is used in the diagnosis and treatment of veterans.	Verbally	Written
Criminal Record Information				
Guardian Information	Paper	Next of kin, DNR instructions, health care proxy designation. This information is used in the notificationprocess and as requried for medical decisions.	Verbally	Written
Education Information	N/A	This information is not collected		
Benefit Information	Paper	Treatment notes, progress notes, clinical assessments, clinical diagnosis information is collected. Used in follow-up treatment and as part of the medical history. C&P examinations are also performed with information input into the CAPRI system utilized by VBA.	Verbally	Written

Other (Explain)	Paper	Next of kin information and emergency contact information, such as name and telephone number is collected from the veteran to use to contact other individuals in case of an emergency. In addition insurance and employment information is available on the veteran for use in billing for care.	Verbally	Written

Data Type	**Is Data Type Stored on your system?**	**Source** (If requested, identify the specific file, entity and/or name of agency)	**Is data collection Mandatory or Voluntary?**	**Additional Comments**
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran	Mandatory	Data used to identify the veteran, determine eligibility for care, schedule treatment, manage healthcare and payment or reimbursement of authorized healthcare
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Voluntary	
Service Information	Yes	Veteran	Mandatory	

Medical Information	Yes	Veteran	Mandatory
Criminal Record Information	No		
Guardian Information	Yes	Veteran	Voluntary
Education Information	No		
Benefit Information	Yes	Veteran	Mandatory
Other (Explain)			
Other (Explain)			
Other (Explain)			

(FY 2011) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	VBA	No	Comp & Pen examinations input into CAPRI templates.	Both PII & PHI	VHA Handbook 1605.1 as referenced by local Privacy Policy
Other Veteran Organization					
Other Federal Government Agency	IRS, SSA, DoD	No	Income verification to	Both PII &	VHA Handbook 1605.1 as
State Government Agency	Medicaid, Licensing Boards, Courts	No	Used to determine eligibility of benefits and identification of authorized patient representatives	Both PII & PHI	VHA Handbook 1605.1 as referenced by local Privacy Policy
Local Government Agency					
Research Entity					
Other Project / System					
Other Project / System					
Other Project / System					

(FY 2011) PIA: Access to Records

Does the system gather information from another system?	No
Please enter the name of the system:	
Per responses in Tab 4, does the system gather information from an individual?	Yes

If information is gathered from an individual, is the information provided:

☑ Through a Written Request
☑ Submitted in Person
☐ Online via Electronic Form

Is there a contingency plan in place to process information when the system is down?	Yes

(FY 2011) PIA: Secondary Use

Will PII data be included with any secondary use request?	No

if yes, please check all that apply: □ Drug/Alcohol Counseling □ Mental Health □ HIV
□ Research □ Sickle Cell □ Other (Please Explain)

Describe process for authorizing access to this data.
Answer:

(FY 2011) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public? No

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Answer:

How is data checked for completeness?

Answer:

What steps or procedures are taken to ensure the data remains current and not out of date?

Answer:

How is new data verified for relevance, authenticity and accuracy?

Answer:

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 2011) PIA: Retention & Disposal

What is the data retention period?

Answer: Clinical information is retained in accordance with VA Records Control Schedule 10-1 which is 75 years after the last episode of patient care.

Explain why the information is needed for the indicated retention period?

Answer: The information is retained for healthcare purposes.

What are the procedures for eliminating data at the end of the retention period?

Answer: The electronic final version of patient medical record is destroyed/deleted 75 years after the last episode of patient care as instructed in VA

Where are these procedures documented?

Answer: Http:/vaww1.va.gov/vapubs/viewPublication.asp?Pub_ID=19&Ftype=2 and VHA Records Control

How are data retention procedures enforced?

Answer: Records Management Responsibilities. The Health Information Resources Service (HIRS) is responsible for developing policies, and

Has the retention schedule been approved by the National Archives and Records Administration (NARA) Yes

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 2011) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13? No

If Yes, How will parental or guardian approval be obtained?

Answer:

(FY 2011) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured. Yes

Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls.. Yes

Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

If 'No' to any of the 3 questions above, please describe why:

Answer:

Is adequate physical security in place to protect against unauthorized access? Yes

If 'No' please describe why:

Answer:

Explain how the project meets IT security requirements and procedures required by federal law.

Answer: A C&A is performed on the system every 3 years with the last one completed in 2010.

Explain what security risks were identified in the security assessment? *(Check all that apply)*

- ☐ Air Conditioning Failure
- ☐ Chemical/Biological Contamination
- ☐ Blackmail
- ☐ Bomb Threats
- ☐ Burglary/Break In/Robbery
- ☑ Cold/Frost/Snow
- ☐ Communications Loss
- ☐ Computer Intrusion
- ☐ Computer Misuse
- ☐ Data Destruction
- ☐ Data Disclosure
- ☐ Data Integrity Loss
- ☐ Denial of Service Attacks
- ☐ Earthquakes
- ☐ Eavesdropping/Interception
- ☐ Errors (Configuration and Data Entry)
- ☑ Fire (False Alarm, Major, and Minor)
- ☑ Flooding/Water Damage
- ☐ Fraud/Embezzlement
- ☑ Hardware Failure
- ☐ Identity Theft
- ☐ Malicious Code
- ☐ Power Loss
- ☐ Sabotage/Terrorism
- ☐ Storms/Hurricanes
- ☐ Substance Abuse
- ☐ Theft of Assets
- ☐ Theft of Data
- ☐ Vandalism/Rioting

Answer: (Other Risks)

Explain what security controls are being used to mitigate these risks. *(Check all that apply)*

☑ Access Control

☑ Audit and Accountability

☑ Awareness and Training

☑ Certification and Accreditation Security Assessments

☑ Configuration Management

☑ Contingency Planning

☑ Identification and Authentication

☑ Incident Response

☑ Media Protection

☑ Personnel Security

☑ Physical and Environmental Protection

☑ Risk Management

Answer: (Other Controls)

PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.

Answer: No choices were made regarding the systems during the performance of the PIA. This has been a fact finding process

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization?
(Choose One)

☑ The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.

□ The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.

□ The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization?
(Choose One)

☑ The potential impact is **high** if the loss of integrity could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.

□ The potential impact is **moderate** if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals.

□ The potential impact is **low** if the loss of integrity could be expected to have a limited adverse effect on operations, assets or individuals.

Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization? **(Choose One)**

☑ The potential impact is **high** if the loss of confidentiality could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.

□ The potential impact is **moderate** if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals.

□ The potential impact is **low** if the loss of confidentiality could be expected to have a limited adverse effect on operations, assets or individuals.

The controls are being considered for the project based on the selections from the previous assessments?

The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

Please add additional controls:

(FY 2011) PIA: Additional Comments

Add any additional comments or information that may have been left out for any question. Please indicate the question you are responding to and then add your comments.

Which of these are sub-components of your system?

Access Manager
Actuarial
Appraisal System
ASSISTS
Awards
Awards
Baker System
Bbraun (CP Hemo)
BDN Payment History
BIRLS
C&P Payment System
C&P Training Website
CONDO PUD Builder
Corporate Database
Data Warehouse
EndoSoft
FOCAS
Inforce
INS - BIRLS
Insurance Online
Insurance Self Service
LGY Home Loans
LGY Processing
Mobilization
Montgomery GI Bill
MUSE
Omnicell
Priv Plus
RAI/MDS
Right Now Web
SAHSHA
Script Pro
SHARE
SHARE
SHARE
Sidexis
Synquest

Automated Sales Reporting (ASR)
BCMA Contingency Machines
Benefits Delivery Network (BDN)
Centralized Property Tracking System
Common Security User Manager (CSUM)
Compensation and Pension (C&P)
Control of Veterans Records (COVERS)
Control of Veterans Records (COVERS)
Control of Veterans Records (COVERS)
Courseware Delivery System (CDS)
Dental Records Manager
Education Training Website
Electronic Appraisal System
Electronic Card System (ECS)
Electronic Payroll Deduction (EPD)
Eligibility Verification Report (EVR)
Fiduciary Beneficiary System (FBS)
Fiduciary STAR Case Review
Financial and Accounting System (FAS)
Insurance Unclaimed Liabilities
Inventory Management System (IMS)
LGY Centralized Fax System
Loan Service and Claims
Loan Guaranty Training Website
Master Veterans Record (MVR)
Mental Health Asisstant
National Silent Monitoring (NSM)
Powerscribe Dictation System
Rating Board Automation 2000 (RBA2000)
Rating Board Automation 2000 (RBA2000)
Rating Board Automation 2000 (RBA2000)
Records Locator System
Review of Quality (ROQ)
Search Participant Profile (SPP)
Spinal Bifida Program Ch 18
State Benefits Reference System
State of Case/Supplemental (SOC/SSOC)

Automated Folder Processing System (AFPS)
Automated Medical Information Exchange II (AIME II)
Automated Medical Information System (AMIS)290
Automated Standardized Performace Elements Nationwide (ASPEN)
Centralized Accounts Receivable System (CARS)
Committee on Waivers and Compromises (COWC)
Compensation and Pension (C&P) Record Interchange (CAPRI)
Compensation & Pension Training Website
Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
Distribution of Operational Resources (DOOR)
Educational Assistance for Members of the Selected Reserve Program CH 1606
Electronic Performance Support System (EPSS)
Enterprise Wireless Messaging System (Blackberry)
Financial Management Information System (FMI)
Hearing Officer Letters and Reports System (HOLAR)
Inquiry Routing Information System (IRIS)
Modern Awards Process Development (MAP-D)
Personnel and Accounting Integrated Data and Fee Basis (PAID)
Personal Computer Generated Letters (PCGL)
Personnel Information Exchange System (PIES)
Personnel Information Exchange System (PIES)
Post Vietnam Era educational Program (VEAP) CH 32
Purchase Order Management System (POMS)
Reinstatement Entitelment Program for Survivors (REAPS)
Reserve Educational Assistance Program CH 1607
Service Member Records Tracking System
Survivors and Dependents Education Assistance CH 35
Systematic Technical Accuracy Review (STAR)
Training and Performance Support System (TPSS)
VA Online Certification of Enrollment (VA-ONCE
VA Reserve Educational Assistance Program
Veterans Appeals Control and Locator System (VACOLS)
Veterans Assistance Discharge System (VADS)
Veterans Exam Request Info System (VERIS)
Veterans Service Representative (VSR) Advisor
Vocational Rehabilitation & Employment (VR&E) CH 31
Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)

VBA Data Warehouse
VBA Training Academy
Veterans Canteen Web
VIC
VR&E Training Website
Web LGY

Telecare Record Manager
VBA Enterprise Messaging System
Veterans On-Line Applications (VONAPP)
Veterans Service Network (VETSNET)
Web Electronic Lender Identification

Web Automated Folder Processing System (WAFPS)
Web Automated Reference Material System (WARMS)
Web Automated Verification of Enrollment
Web-Enabled Approval Management System (WEAMS)
Web Service Medical Records (WebSMR)
Work Study Management System (WSMS)

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Which of these are sub-components of your system?

x ASISTS
x Bed Control
x CAPRI
x CMOP
x Dental
x Dietetics
x Fee Basis
x GRECC
x HINQ
x IFCAP
x Imaging
x Kernal
x Kids
x Lab Service
x Letterman
x Library
x Mailman
x Medicine
x MICOM
x NDBI
x NOIS
x Oncology
x PAID
x Prosthetics
x QUASER
x RPC Broker
x SAGG
x Scheduling
x Social Work
x Surgery
x Toolkit
x Unwinder
x VA Fileman
x VBECS
x VDEF
x VistALink

x Beneficiary Travel
x Care Management
x Care Tracker
x Clinical Reminders
x CPT/ HCPCS Codes
x DRG Grouper
x DSS Extracts
x Education Tracking
x Engineering
x Event Capture
x Extensible Editor
x Health Summary
x Incident Reporting
x Intake/ Output
x Integrated Billing
x Lexicon Utility
x List Manager
x Mental Health
x MyHealthEVet
x National Drug File
x Nursing Service
x Occurrence Screen
x Patch Module
x Patient Feedback
x Police & Security
x Problem List
x Progress Notes
x Record Tracking
x Registration
x Run Time Library
x Survey Generator
x Utilization Review
x Visit Tracking
x VistALink Security
x Women's Health

x Accounts Receivable
x ADP Planning (PlanMan)
x Bad Code Med Admin
x Clinical Case Registries
x Clinical Procedures
x Consult/ Request Tracking
x Controlled Substances
x Credentials Tracking
x Discharge Summary
x Drug Accountability
x EEO Complaint Tracking
x Electronic Signature
x Event Driven Reporting
x External Peer Review
x Functional Independence
x Gen. Med. Rec. - I/O
x Gen. Med. Rec. - Vitals
x Generic Code Sheet
x Health Level Seven
x Hospital Based Home Care
x Inpatient Medications
x Integrated Patient Funds
x MCCR National Database
x Minimal Patient Dataset
x National Laboratory Test
x Network Health Exchange
x Outpatient Pharmacy
x Patient Data Exchange
x Patient Representative
x PCE Patient/ HIS Subset
x Security Suite Utility Pack
x Shift Change Handoff Tool
x Spinal Cord Dysfunction
x Text Integration Utilities
x VHS & RA Tracking System
x Voluntary Timekeeping

x Adverse Reaction Tracking
x Authorization/ Subscription
x Auto Replenishment/ Ward Stock
x Automated Info Collection Sys
x Automated Lab Instruments
x Automated Med Info Exchange
x Capacity Management - RUM
x Capacity Management Tools
x Clinical Info Resource Network
x Clinical Monitoring System
x Enrollment Application System
x Equipment/ Turn-in Request
x Gen. Med.Rec. - Generator
x Health Data and Informatics
x ICR - Immunology Case Registry
x Income Verification Match
x Incomplete Records Tracking
x Interim Mangement Support
x Master Patient Index VistA
x Missing Patient Reg (Original) A4EL
x Order Entry/ Results Reporting
x PCE Patient Care Encounter
x Pharmacy Benefits Mangement
x Pharmacy Data Management
x Pharmacy National Database
x Pharmacy Prescription Practice
x Quality Assurance Integration
x Quality Improvement Checklist
x Radiology/ Nuclear Medicine
x Release of Information - DSSI
x Remote Order/ Entry System
x Utility Management Rollup
x CA Vertified Components - DSSI
x Vendor - Document Storage Sys
x Visual Impairment Service Team ANRV
x Voluntary Timekeeping National

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

(FY 2011) PIA: Minor Applications

Which of these are sub-components of your system?

1184 Web

A4P

ENDSOFT

Enterprise Terminology Server & VHA Enterprise Terminology Services

RAFT

RALS

(FY 2011) PIA: Final Signatures

Facility Name: Region 1>VHA>VISN 19>Sheridan VAMC>VistA

Title:	Name:	Phone:	Email:
Privacy Officer:	Jamie Banks	307.675.3611	jamie.banks@va.gov
Digital Signature Block			
Information Security Officer:	Doug Bohnenblust	307.675.3880	douglas.bohnenblust@va.gov
Digital Signature Block			
System Owner/ Chief Information Officer:	Cynthia Sostrom	307.675.3143	cynthia.sostrom@va.gov
Digital Signature Block			
Information Owner:	0	0	0
Digital Signature Block			
Other Titles:	0	0	0
Digital Signature Block			

Date of Report:	1/0/00
OMB Unique Project Identifier	029-00-01-11-01-1180-00
Project Name	Region 1>VHA>VISN 19>Sheridan VAMC>VistA